



**WORLD INTELLECTUAL PROPERTY ORGANIZATION
ORGANISATION MONDIALE DE LA PROPRIÉTÉ INTELLECTUELLE**

34, chemin des Colombettes, Case postale 18, CH-1211 Genève 20 (Suisse)
Téléphone: (41 22) 338 91 11 - e-mail: wipo.mail @ wipo.int. - Fac-similé: (41 22) 733 54 28

**PATENT COOPERATION TREATY (PCT)
TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)**

**CERTIFIED COPY OF THE INTERNATIONAL APPLICATION AS FILED
AND OF ANY CORRECTIONS THERETO**

**COPIE CERTIFIÉE CONFORME DE LA DEMANDE INTERNATIONALE, TELLE QU'ELLE
A ÉTÉ DÉPOSÉE, AINSI QUE DE TOUTES CORRECTIONS Y RELATIVES**

International Application No. } **PCT/IB02/04450**
Demande internationale n° }

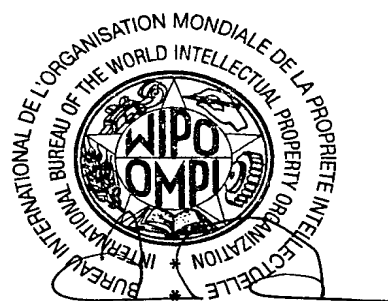
International Filing Date } **28 October 2002**
Date du dépôt international } **(28.10.02)**

Geneva/Genève,

**25 September 2003
(25.09.03)**

**International Bureau of the
World Intellectual Property Organization (WIPO)**

**Bureau International de l'Organisation Mondiale
de la Propriété Intellectuelle (OMPI)**



J.-L. Baron

**Head, PCT Receiving Office Section
Chef de la section "office récepteur du PCT"**

PCT REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty

For receiving Office use only	
PCT / IB 0 2 / 0 4 4 5 0	
International Application No.	
28 OCTOBER 2002	(28. 10. 02)
International Filing Date	
INTERNATIONAL BUREAU OF WIPO	
Name of receiving Office and "PCT International Application"	
Applicant's or agent's file reference (if desired)(12 characters maximum)	2018604

Box No. I TITLE OF INVENTION	
DEVICE KEYS	
Box No. II APPLICANT <input type="checkbox"/> This person is also inventor.	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)	Telephone No.
Nokia Corporation	Facsimile No.
Keilalahdentie 4	Teleprinter No.
FI- 02150 ESPOO	Applicant's registration No. with the Office
FINLAND	
State (that is, country) of nationality: FI	State (that is, country) of residence: FI
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input checked="" type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box	
Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)	This person is:
ASOKAN, N	<input type="checkbox"/> applicant only
Ankkurinvarsi 6 K	<input checked="" type="checkbox"/> applicant and inventor
FIN-02320 ESPOO	<input type="checkbox"/> inventor only (if this check-box is marked, do not fill in below.)
FINLAND	Applicant's registration No. with the Office
State (that is, country) of nationality: CA	State (that is, country) of residence: FI
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input checked="" type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box	
<input checked="" type="checkbox"/> Further applicants and/or (further) inventors are indicated on a continuation sheet	
Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE	
The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: <input checked="" type="checkbox"/> agent <input type="checkbox"/> common representative	
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)	Telephone No.
AWAPATENT AB	+46 8 440 95 00
BOX 45086	Facsimile No.
SE-104 30 STOCKHOLM	+46 8 440 95 50
SWEDEN	Teleprinter No.
	Agent's registration No. with the Office
<input type="checkbox"/> Address for correspondence: Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent	

Sheet No. 2

Continuation of Box No. III		FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)	
<i>If none of the following sub-boxes is used, this sheet should not be included in the request.</i>			
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.) NIEMI, Valtteri Tallberginkatu 3 as 43 FIN-00180 Helsinki FINLAND		This person is: <input type="checkbox"/> applicant only <input checked="" type="checkbox"/> applicant and inventor <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.) Applicant's registration No. with the Office	
State (that is, country) of nationality: FI		State (that is, country) of residence: FI	
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input checked="" type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box			
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)		This person is: <input type="checkbox"/> applicant only <input type="checkbox"/> applicant and inventor <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.) Applicant's registration No. with the Office	
State (that is, country) of nationality:		State (that is, country) of residence:	
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box			
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)		This person is: <input type="checkbox"/> applicant only <input type="checkbox"/> applicant and inventor <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.) Applicant's registration No. with the Office	
State (that is, country) of nationality:		State (that is, country) of residence:	
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box			
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)		This person is: <input type="checkbox"/> applicant only <input type="checkbox"/> applicant and inventor <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.) Applicant's registration No. with the Office	
State (that is, country) of nationality:		State (that is, country) of residence:	
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box			
Name and address: (Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)		This person is: <input type="checkbox"/> applicant only <input type="checkbox"/> applicant and inventor <input type="checkbox"/> inventor only (If this check-box is marked, do not fill in below.) Applicant's registration No. with the Office	
State (that is, country) of nationality:		State (that is, country) of residence:	
This person is applicant for the purposes of: <input type="checkbox"/> all designated States <input type="checkbox"/> all designated States except the United States of America <input type="checkbox"/> the United States of America only <input type="checkbox"/> the States indicated in the Supplemental Box			
<input type="checkbox"/> Further applicants and/or (further) inventors are indicated on another continuation sheet.			

Form PCT/RO/101 (continuation sheet) (March 2001; reprint January 2002)

See Notes to the request form

Sheet No. 3

Box No. V	DESIGNATION OF STATES	Mark the applicable check-boxes below; at least one must be marked.
The following designations are hereby made under Rule 4.9(a):		
Regional Patent		
<input checked="" type="checkbox"/> AP	ARIPO Patent: GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, MZ Mozambique, SD Sudan, SL Sierra Leone, SZ Swaziland, TZ United Republic of Tanzania, UG Uganda, ZM Zambia, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT (if other kind of protection or treatment desired, specify on dotted line)	
<input checked="" type="checkbox"/> EA	Eurasian Patent: AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT	
<input checked="" type="checkbox"/> EP	European Patent: AT Austria, BE Belgium, CH and LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, TR Turkey, and any other State which is a Contracting State of the European Patent Convention and of the PCT	
<input checked="" type="checkbox"/> OA	OAPI Patent: BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT (if other kind of protection or treatment desired, specify on dotted line)	
National Patent (if other kind of protection or treatment desired, specify on dotted line):		
<input checked="" type="checkbox"/> AE	United Arab Emirates	<input checked="" type="checkbox"/> GM Gambia
<input checked="" type="checkbox"/> AG	Antigua and Barbuda	<input checked="" type="checkbox"/> HR Croatia
<input checked="" type="checkbox"/> AL	Albania	<input checked="" type="checkbox"/> HU Hungary
<input checked="" type="checkbox"/> AM	Armenia	<input checked="" type="checkbox"/> ID Indonesia
<input checked="" type="checkbox"/> AT	Austria +Utility Model	<input checked="" type="checkbox"/> IL Israel
<input checked="" type="checkbox"/> AU	Australia	<input checked="" type="checkbox"/> IN India
<input checked="" type="checkbox"/> AZ	Azerbaijan	<input checked="" type="checkbox"/> IS Iceland
<input checked="" type="checkbox"/> BA	Bosnia and Herzegovina	<input checked="" type="checkbox"/> JP Japan
<input checked="" type="checkbox"/> BB	Barbados	<input checked="" type="checkbox"/> KE Kenya
<input checked="" type="checkbox"/> BG	Bulgaria	<input checked="" type="checkbox"/> KG Kyrgyzstan
<input checked="" type="checkbox"/> BR	Brazil	<input checked="" type="checkbox"/> KP Democratic People's Republic of Korea
<input checked="" type="checkbox"/> BY	Belarus	<input checked="" type="checkbox"/> KR Republic of Korea
<input checked="" type="checkbox"/> BZ	Belize	<input checked="" type="checkbox"/> KZ Kazakhstan
<input checked="" type="checkbox"/> CA	Canada	<input checked="" type="checkbox"/> LC Saint Lucia
<input checked="" type="checkbox"/> CH & LI	Switzerland and Liechtenstein	<input checked="" type="checkbox"/> LK Sri Lanka
<input checked="" type="checkbox"/> CN	China	<input checked="" type="checkbox"/> LR Liberia
<input checked="" type="checkbox"/> CO	Colombia	<input checked="" type="checkbox"/> LS Lesotho
<input checked="" type="checkbox"/> CR	Costa Rica	<input checked="" type="checkbox"/> LT Lithuania
<input checked="" type="checkbox"/> CU	Cuba	<input checked="" type="checkbox"/> LU Luxembourg
<input checked="" type="checkbox"/> CZ	Czech Republic +Utility Model	<input checked="" type="checkbox"/> LV Latvia
<input checked="" type="checkbox"/> DE	Germany +Utility Model	<input checked="" type="checkbox"/> MA Morocco
<input checked="" type="checkbox"/> DK	Denmark +Utility Model	<input checked="" type="checkbox"/> MD Republic of Moldova
<input checked="" type="checkbox"/> DM	Dominica	<input checked="" type="checkbox"/> MG Madagascar
<input checked="" type="checkbox"/> DZ	Algeria	<input checked="" type="checkbox"/> MK The former Yugoslav Republic of Macedonia
<input checked="" type="checkbox"/> EC	Ecuador	<input checked="" type="checkbox"/> MN Mongolia
<input checked="" type="checkbox"/> EE	Estonia +Utility Model	<input checked="" type="checkbox"/> MW Malawi
<input checked="" type="checkbox"/> ES	Spain	<input checked="" type="checkbox"/> MX Mexico
<input checked="" type="checkbox"/> FI	Finland +Utility Model	<input checked="" type="checkbox"/> MZ Mozambique
<input checked="" type="checkbox"/> GB	United Kingdom	<input checked="" type="checkbox"/> NO Norway
<input checked="" type="checkbox"/> GD	Grenada	
<input checked="" type="checkbox"/> GE	Georgia	
<input checked="" type="checkbox"/> GH	Ghana	
<input checked="" type="checkbox"/> NZ	New Zealand	
<input checked="" type="checkbox"/> OM	Oman	
<input checked="" type="checkbox"/> PH	Philippines	
<input checked="" type="checkbox"/> PL	Poland	
<input checked="" type="checkbox"/> PT	Portugal	
<input checked="" type="checkbox"/> RO	Romania	
<input checked="" type="checkbox"/> RU	Russian Federation	
<input checked="" type="checkbox"/> SD	Sudan	
<input checked="" type="checkbox"/> SE	Sweden	
<input checked="" type="checkbox"/> SG	Singapore	
<input checked="" type="checkbox"/> SI	Slovenia	
<input checked="" type="checkbox"/> SK	Slovakia +Utility Model	
<input checked="" type="checkbox"/> SL	Sierra Leone	
<input checked="" type="checkbox"/> TJ	Tajikistan	
<input checked="" type="checkbox"/> TM	Turkmenistan	
<input checked="" type="checkbox"/> TN	Tunisia	
<input checked="" type="checkbox"/> TR	Turkey	
<input checked="" type="checkbox"/> TT	Trinidad and Tobago	
<input checked="" type="checkbox"/> TZ	United Republic of Tanzania	
<input checked="" type="checkbox"/> UA	Ukraine	
<input checked="" type="checkbox"/> UG	Uganda	
<input checked="" type="checkbox"/> US	United States of America	
<input checked="" type="checkbox"/> UZ	Uzbekistan	
<input checked="" type="checkbox"/> VN	Viet Nam	
<input checked="" type="checkbox"/> YU	Yugoslavia	
<input checked="" type="checkbox"/> ZA	South Africa	
<input checked="" type="checkbox"/> ZM	Zambia	
<input checked="" type="checkbox"/> ZW	Zimbabwe	
Check-boxes below reserved for designating States which have become party to the PCT after issuance of this sheet:		
<input checked="" type="checkbox"/>		
<input type="checkbox"/>		
Precautionary Designation Statement: In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that these additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. (Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)		

Form PCT/RO/101 (second sheet) (January 2002)

See Notes to the request form

Sheet No. 4

Box No. VI PRIORITY CLAIM				
The priority of the following earlier application(s) is hereby claimed:				
Filing date of earlier application (day/month/year)	Number of earlier application	Where earlier application is:		
		national application: country	regional application:* regional Office	international application: receiving Office
item (1) ---	---			
item (2)				
item (3)				
item (4)				
item (5)				

☐ Further priority claims are indicated in the Supplemental Box.

The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) (only if the earlier application was filed with the Office which for the purposes of this international application is the receiving Office) identified above as:

☐ all items ☐ item (1) ☐ item (2) ☐ item (3) ☐ item (4) ☐ item (5) ☐ other, see Supplemental Box

* Where the earlier application is an ARIPO application, indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed (Rule 4.10(b)(ii)):

Box No. VII INTERNATIONAL SEARCHING AUTHORITY

Choice of International Searching Authority (ISA) (if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used):

ISA / EP

Request to use results of earlier search; reference to that search (if an earlier search has been carried out by or requested from the International Searching Authority):

Date (day/month/year)

Number

Country (or regional Office)

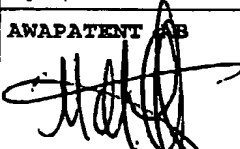
Box No. VIII DECLARATIONS

The following declarations are contained in Boxes Nos. VIII (i) to (v) (mark the applicable check-boxes below and indicate in the right column the number of each type of declaration):

Number of
declarations

- | | | |
|---|--|---|
| <input type="checkbox"/> Box No. VIII (i) | Declaration as to the identity of the inventor | : |
| <input type="checkbox"/> Box No. VIII (ii) | Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent | : |
| <input type="checkbox"/> Box No. VIII (iii) | Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application | : |
| <input type="checkbox"/> Box No. VIII (iv) | Declaration of inventorship (only for the purposes of the designation of the United States of America) | : |
| <input type="checkbox"/> Box No. VIII (v) | Declaration as to non-prejudicial disclosures or exceptions to lack of novelty | : |

Sheet No. 5

Box No. IX CHECK LIST, LANGUAGE OF FILING	
<p>This international application contains:</p> <p>(a) the following number of sheets in paper form:</p> <p>request (including declaration sheets) : 5</p> <p>description (excluding sequence listing part) : 17</p> <p>claims : 7</p> <p>abstract : 1</p> <p>drawings : 2</p> <p>Sub-total number of sheets : 32</p> <p>sequence listing part of description (<i>actual number of sheets if filed in paper form, whether or not also filed in computer readable form; see (b) below</i>) :</p> <p>Total number of sheets : 32</p> <p>(b) sequence listing part of description filed in computer readable form</p> <p>(i) <input type="checkbox"/> only (under Section 801(a)(i))</p> <p>(ii) <input type="checkbox"/> in addition to being filed in paper form (under Section 801(a)(ii))</p> <p>Type and number of carriers (diskette, CD-ROM, CD-R or other) on which the sequence listing part is contained (<i>additional copies to be indicated under item 9(ii), in right column</i>):</p>	<p>This international application is accompanied by the following item(s) (mark the applicable check-boxes below and indicate in right column the number of each item):</p> <p>1. <input type="checkbox"/> fee calculation sheet : _____</p> <p>2. <input type="checkbox"/> original separate power of attorney : _____</p> <p>3. <input type="checkbox"/> original general power of attorney : _____</p> <p>4. <input type="checkbox"/> copy of general power of attorney; reference number, if any: _____ : _____</p> <p>5. <input type="checkbox"/> statement explaining lack of signature : _____</p> <p>6. <input type="checkbox"/> priority document(s) identified in Box No. VI as item(s): _____ : _____</p> <p>7. <input type="checkbox"/> translation of international application into (language): _____ : _____</p> <p>8. <input type="checkbox"/> separate indications concerning deposited microorganism or other biological material : _____</p> <p>9. <input type="checkbox"/> sequence listing in computer readable form (indicate also type and number of carriers (diskette, CD-ROM, CD-R or other))</p> <p>(i) <input type="checkbox"/> copy submitted for the purposes of international search under Rule 13ter only (and not as part of the international application) : _____</p> <p>(ii) <input type="checkbox"/> (only where check-box (b)(i) or (b)(ii) is marked in left column) additional copies including, where applicable, the copy for the purposes of international search under Rule 13ter : _____</p> <p>(iii) <input type="checkbox"/> together with relevant statement as to the identity of the copy or copies with the sequence listing part mentioned in left column : _____</p> <p>10. <input type="checkbox"/> other (<i>specify</i>): _____ : _____</p>
Figure of the drawings which should accompany the abstract: 1	Language of filing of the international application: ENGLISH
Box No. X SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE	
Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).	
<p>AWAPATENT AB</p>  <p>Mats Lindgren</p> <p>Authorised agent</p>	

For receiving Office use only	
1. Date of actual receipt of the purported international application: 28 OCTOBER 2002	2. Drawings: <input type="checkbox"/> received: <input type="checkbox"/> not received:
3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:	
4. Date of timely receipt of the required corrections under PCT Article 11(2):	
5. International Searching Authority (if two or more are competent): ISA EP	6. <input checked="" type="checkbox"/> Transmittal of search copy delayed until search fee is paid.

Date of receipt of the record copy by the International Bureau:

For International Bureau use only

Form PCT/RO/101 (last sheet) (March 2001; reprint January 2002)

See Notes to the request form

DEVICE KEYSTechnical field of the invention

The present invention relates to key management of cryptographic keys, which keys are intended to be used by applications included in a personal device.

5

Technical background and prior art

The use of personal devices, such as cellular telephones and hand-held PDA:s (Personal Digital Assistant), is becoming increasingly popular. Other kind
10 of personal devices, including any mobile communication terminal having a terminal identity which somehow is associated with an end user identity, or in possession of an anonymous user, are easily conceivable. Among the end users of the personal devices and the parties
15 communicating with these devices there is a need to be able to use encrypted communication, digital signatures and digital certificates. With these kind of cryptographic techniques it is possible to ensure secrecy and integrity of communicated information data,
20 authenticate an originator of information, as well as authenticating an intended recipient of information.

Encrypted communication between two entities is typically based on either shared secret keys or on public/private key pairs. To implement key-based
25 encrypted communication and/or the use of digital signatures, schemes are needed to determine how and where the required keys should be generated, and also how to distribute the generated keys to the involved entities. A more general term which includes issues regarding
30 generation, storage and distribution of keys, and which also is used in this document, is key management.

Secret keys obviously have to be managed and somehow be distributed among the participating entities. If a

2

secret or private key should be transferred to an entity it is important that this is performed in a secure way such that the key is not exposed to a third party, even if such a third party would do its utmost to get access to such a key. Public/private key pairs may be generated within an entity, requiring that only the public key needs to be distributed outside the entity. However, in case the public/private key pair is generated outside the specific entity, the private key needs to be transferred to the entity. Whenever a secret or private key is transferred it is also important to be able to ensure integrity of the key.

Future personal devices will include one or more device specific cryptographic keys. The number and types of these keys are dependent on the different applications included in the device, which applications will differ between different users and their respective usage of the device. Thus, it is difficult to foresee these numbers and types of keys that should be included in the device. For this reason it is necessary to be able to store a variety of keys in a storage area of the device when initializing the device. Typically, most of these keys will be stored in some non-robust memory, i.e. any memory in which information can be written and with the potential risk of losing any such information due to failure of the mechanism used for maintaining the information in the memory. As a consequence, in case of a failure of the device that results in loss of the originally stored keys, it is desired to be able to restore these original keys in a device. When transferring any secret or private keys for re-storage in the device, it is typically required, as discussed above, to maintain secrecy and integrity of the transferred keys.

US patent 5,892,900, assigned to Intertrust, discloses, among other things, the use of cryptographic keys for providing security to cryptographic key

- management. The document describes a "Secure Processing Unit" (SPU) with a "Protected Processing Environment" (PPE) designed to perform processing tasks and to communicate with external entities in a secure manner.
- 5 The PPE contains a key storage that is initialized with keys generated by the manufacturer and by the PPE itself. A manufacturing key that is public-key based or based on a shared secret is used as a so called master key for communicating other keys in a secure way. The
- 10 manufacturing key is either hardwired into the PPE at manufacturing time, or sent to the PPE as its first key. The manufacturing key is used for protecting various other keys downloaded in the PPE, such as a public/private key pair and/or secret shared keys.
- 15 Alternatively, the PPE has the capability of generating its own key pairs internally, in which case a manufacturing key may not be needed.

- Disclosed in US, 5,892,900 is also the use of a download authorization key. The download authorization
- 20 key is received by the PPE during an initialization download process. It is used to authorize PPE key updates and to protect a PPE external secure database backup to allow recovery by an administrator of the PPE if the PPE fails. The document also discloses the use of backup
- 25 keys. A backup key is generated and stored within the PPE. A secure database external to the PPE stores backup records encrypted with the backup key. The backup key may be encrypted with the download authentication key and stored within the backup itself to permit an
- 30 administrator to decrypt and recover the backup in case of PPE failure.

Summary of the invention

- An object of the invention is to provide a method
- 35 and a system for managing, with reduced overhead, cryptographic keys that are specific to a personal device.

tion is to
device specific
with improved
of US 5,892,900

these objects
independent claim
claim 9 and a
preferred
claims.
package including
ferred to a
point of a
device specific
e. In response to
data package is
from the personal
data package
stored in a
p included in the
point retrieves a
i associates the
after which the
associated unique
, global public
.

ground section,
stored in some
memory, of the
y is lost or
red using the
there will be no
storing keys to
ges. Instead, the
package is
ble to decrypt a

18604\20021022 Filed

5

received backup data package using the unique secret chip key for the purpose of restoring the cryptographic keys.

Neither the device manufacturer nor any device administrator needs to maintain a secret database storing
5 keys for decrypting backup data packages. In fact, it is preferred, for security reasons, not to store or distribute any copies of the unique secret chip key at chip manufacturing. This unique secret chip key never leaves the tamper-resistant storage. No other entity,
10 including the device manufacturer, ever learns this key. Besides enabling improved security this also greatly simplifies key management.

By storing the backup data packages in a public database, key management is further simplified and made
15 less costly. Moreover, this allows not only a device manufacturer but anyone in control of the device, such as a device owner or device administrator, to completely on its own restore the original cryptographic keys of a device.

20 The encryption and decryption of a backup data package within the device, using the non-distributed unique secret chip key stored in the device, provide protection and integrity of the backup data package content, both during transfer and storage in the public
25 database. As is understood, the data package may include any kind of cryptographic keys for various purposes, e.g. keys relating to DRM(Digital Rights Management), SIM(Subscriber Identity Module) locking of a personal device implementing a wireless terminal, the provision of
30 a secure, key based communication channel between the personal device and the device manufacturer etc. Furthermore, any other kind of secret, device specific information may also be included in the data package and, thus, be protected by the unique secret chip key in the
35 same way as the cryptographic keys. Thus, the information included in the backup data package stored in the public

6

database may relate to cryptographic keys as well as other secret, device specific data.

Advantageously, the backup data package includes one or more communication keys for a secure, key based communication between the device manufacturer and the device. This means that the establishment and recovery of such a secure communication channel will be protected and provided with integrity. That is, an external party will not be able to alter the communication key of the secure channel for the device so that the encryption/decryption of this secure channel determined during assembly is circumvented, for example if the device were to be stolen or re-distributed on another consumer market by a dishonest possessor of a device. This ensures a secure channel for communication between the manufacturer and the personal device, which communication can not be tampered with by any device owner or third party, both during the process of device assembly and after the personal device has been shipped to a customer.

Preferably, a certificate for the unique device identity associated with a specific device is stored in association with the corresponding backup data package. This has the advantage that the unique device identity may be verified, by means of a public signature verification key stored in a ROM memory of the device, as the authentic device identity during recovery of the personal device.

The one or more cryptographic keys in the data package advantageously include symmetric and/or public/private keys necessary for any subsequent secure communication between the device and its manufacturer, not excluding other cryptographic keys for other communication purposes, such as encryption key pairs and signature key pairs.

The keys in the data package are either provided to the secure processing point from an external source or generated by the secure processing point itself. This

means that there is no deterministic generation within the device of the cryptographic keys to be used for communication with the manufacturer. This provides flexibility in deciding what implementation, with respect

5 to type of cryptographic keys and algorithms, to choose for, e.g., the secure communication channel. Also, keys and algorithms for such a secure communication channel can be changed when necessary, without having to change the basic manufacturing/assembly process.

10 Furthermore, by minimizing, or completely avoiding, public key generation internally in the device, the computations within the device are minimized. This reduced overhead provides smaller delays and faster assembly of the device on the assembly line.

15 Thus, the present invention simplifies and reduces the overhead for both assigning device specific cryptographic keys to a personal device as well as managing these cryptographic keys after assembly and shipment of the device.

20 Further features and advantages of the invention will become more readily apparent from the following detailed description.

Brief description of the drawings

25 Exemplifying embodiments of the present invention will be described in greater detail with reference to the accompanying drawings, in which the same features appearing in several drawings have been denoted with the same reference signs, and in which:

30 Fig. 1 schematically shows an exemplifying system which includes the elements and illustrates the operation of preferred embodiments of the invention; and

Fig. 2 schematically illustrates some possible device management activities that can be performed after

35 shipment of the device assembled in Fig. 1.

Detailed description of preferred embodiments

With reference to Fig.1 an exemplifying embodiment of the invention will now be described in greater detail. Shown in the figure is a personal device 100 subject to assembly at a device manufacturer. The manufacturer controls the assembly of the device by means of a secure processing point 150 which is arranged in communication with the device. The method and means for communicating with the device can be based on any technique that is known to the skilled person and that is suitable for the type of device in question. As will be appreciated by a person skilled in the art, the assembly of the device will initially include loading of various basic software modules in a memory of the device, such as I/O-drivers and a communication protocol to be used by interface circuitry of the device for implementing a communication port (not shown). Alternatively, such I/O-drivers may already be stored in a ROM memory (not shown) included by the device. The secure processing point 150 will include corresponding communications software that is compatible with the communication protocol used by the communication port of the device, thus facilitating communication between the secure processing point 150 and the personal device 100.

The implementation of the personal device 100 is based on a hardware platform that includes all kinds of circuitry needed for the personal device to be able to operate, such as memory circuitry, processing circuitry, interfacing circuitry etc. Of importance with respect to the invention, the device 100 includes an integrated chip 110, which chip includes a read-only storage area 120 and a tamper-resistant secret storage 125. The chip can be designed using any state of the art technique, subject to the condition that these two storage areas are provided within the chip. The device also includes a memory circuit 130, providing an ordinary non-secure memory, e.g. implemented by a flash memory, in which information

may be written. Furthermore, the device includes means 127 for encrypting data which are received in a data package, i.e. a package defining a collection of data, from the secure processing point, using a unique secret chip key stored in the tamper-resistant secret storage 125. This means for encrypting a received data package is implemented by any suitable processing hardware means, such as a microprocessor or one or more application specific integrated circuits, executing program instructions which have been loaded into a memory of the device. This execution causes the processing hardware to perform symmetric encryption of the data in accordance with known techniques. Consequently, the design of these program instructions will be appreciated by a person skilled in the art of programming.

The secure processing point 150 includes processing means 155, e.g. by means of a general purpose computer implementation, for controlling the communication with the device and for performing certain activities with respect to a device. The processing means 155 also facilitates communication with various databases 140, 160 and 170, to which the secure processing point 150 is operatively connected. The processing means 155 controls the secure processing point 150 to operate in accordance with the present invention by executing suitable program instructions. The design of these program instructions will be appreciated by a person skilled in the art of programming after having studied the description of the operation of the invention as set forth below.

A temporary secure database 140 is provided as storage for unique device identities that are used in a first embodiment of the invention. The type of identities stored depend on the type of devices subject to assembly. If the devices are wireless communications terminals to be used in a wireless communications network, for example as Mobile Stations in a GSM network (Global System for Mobile communications) or as User Equipments in a UMTS

10

network (Universal Mobile Telecommunications System), the unique device identities will correspond to International Mobile Equipment Identities (IMEIs). The secure database 140 may also be provided as storage for symmetric keys or private/public key pairs that have been derived in advance, i.e. before assembly of the devices in which the symmetric keys or private/public key pairs are to be stored by means of data packages. As stated, the database 140 is temporary. After information has been retrieved from this database with respect to a device, this information is deleted from the database.

The system shown in Fig. 1 also includes a permanent public database 170 for storing backup data packages received from the secure processing point, which backup data packages constitute data packages encrypted by respective devices. Furthermore, the system may also include an optional secret database 160, which belong to the manufacturer and in which the manufacturer may store certain device specific data of the devices that have been assembled.

Referring again to Fig. 1, an exemplifying mode of operation of the system and its included embodiment of the invention will now be described. The description particularly emphasizes on the activities performed for managing cryptographic keys in accordance with the described embodiment, which activities will be described in a step by step fashion. To illustrate the element interactions and data flow involved in the various steps, arrows having numbers corresponding to the steps have been included in the figure.

Initially, in step 1, and as indicated with arrow 1, the device manufacturer receives the hardware on which the personal device is to be based from a factory producing such hardware. As explained above, the hardware includes the integrated chip 110, with its read-only storage area 120 and tamper-resistant secret storage 125, and the memory circuit 130. The assembly of the device

starts in step 2 by downloading various basic executable software modules in the device from the secure processing point 150, as indicated with arrow 2. Alternatively, or in addition, some basic software modules may already be stored in a ROM memory included by the device. In particular, program instructions for controlling the processing means 127 of the device to operate so as to implement the means for encrypting a data package are stored in the memory circuit 130. The stored instructions also includes instructions for decrypting a received backup data package.

In step 3, a unique device identity may be retrieved by the secure processing point 150 from the database 140 storing a number of unique device identities. As a further option, this step may also include retrieving a symmetric key or one or more private/public key pairs that have been generated or computed in advance.

In step 4 the secure processing point 150 retrieves a unique chip identifier from the read-only storage area 120 of the integrated chip 110 included by the device 100 currently being subject to assembly. The secure processing point then assembles a data package which is to be stored in the device 100 in question. This data package should include at least one cryptographic key in order to enable, e.g., future secure, key based communication between the personal device 100 and the personal device manufacturer over a, for the purpose, suitably established communication channel between the same.

The at least one cryptographic key which, e.g., is associated with the future secure communication channel may either be a symmetric key or a public/private key pair. As previously described, the key or key pair may either be provided from an external source, implemented by the secure database 140, or optionally be generated by the secure processing point itself.

If a symmetric key is used, the secure processing point may generate this key as a function of one single secret master key and the unique device identity. By deriving the symmetric keys from the respective unique device identities, it will not be necessary to store all symmetric keys for all devices in a secret database, neither during the assembly process nor afterwards when the symmetric keys are to be used during communication with an assembled device over the secure communication channel. The only key that needs to be secretly stored is the master key common for all symmetric keys.

If a public/private key pair is used the generation of this pair outside of the device will, as previously described, speed up the assembly process. Any generation of the key pair in the secure processing point will be performed in accordance with known techniques. If this key pair, and a certificate for the public key of the key pair, are computed in advance and provided by an external source, implemented as secure database 140, the speed of the device assembly will be even faster. As will be clear to a person skilled in the art, the private key and the public key for the certificate is stored in a device by incorporating them in a data package. The public key corresponding to the private key and its certificate can then be stored in a database, such as database 170, without taking any particular security measures. After these storage operations the generated key and certificate information can be removed from the database 140. In this way the necessity of any on-line secret database for the public/private key pair will be avoided. In comparison with using a symmetric key generated by the secure processing point, the use of a key pair will avoid the necessity to secretly store a master key from which the symmetric keys are derived.

In step 5 the data package, which includes at least a symmetric key or a public/private key pair, is subject to encryption by the device and loaded in the memory

13

circuit 130 of the device 100. Upon reception of the data package, the processing means 127 of the device will use the unique secret chip key from the secret storage 125 for encrypting, a part of or the full content of, the received data package. The encryption is performed by execution of appropriate program instructions, designed in accordance with known techniques, which previously have been loaded in the device (in step 2).

In step 6 the secure processing point receives a backup data package from the device, which backup data package is equal to the data package content that has been encrypted with the unique secret chip key of the device. The secure processing point may now add a backup code to the backup data package in order for the device to in the future, upon reception, be able to distinguish the backup data package from an ordinary data package. Alternatively, such code can be added to the backup data package by the device itself. Of course, other ways of implementing this distinguishing mechanism will be appreciated by the skilled person. The secure processing point associates the unique chip identifier, retrieved in step 4, with the received backup data package.

According to an embodiment of the invention, each device has a corresponding unique device identity. Furthermore, this unique device identity should be stored in the device together with a certificate for the unique device identity. As described above, the secure processing point 150 will in this case retrieve (in step 3) a unique device identity from the secure database 140. Furthermore, step 4 above will include associating the retrieved unique device identity with the retrieved unique chip identifier, e.g. by performing a concatenation of the two. Then the result of the concatenation is signed using a private signature key of the manufacturer. This private signature key corresponds to a public signature key of the manufacturer which public key has been stored in a read-only memory of the

14

device, e.g. in step 2 above. The resulting certificate for the unique device identity is stored in the flash memory of the device in step 5 above. In step 6 the association of the unique chip identifier with the received backup data package also includes the association of the unique device identity and its generated certificate.

In step 7 various device specific data may be stored in an database 160 administrated by the manufacturer. The security level of this database 160 depends on the kind of data stored therein. Typically, the data included therein are data that are used when offering various services to a third party with respect to the device, which data only requires a moderate level of security. However, this database will constitute an on-line secret database with high security in those cases such a high security database is required, e.g. for storing symmetric keys or a master secret key for the generation of symmetric keys.

In step 8 the backup data package and the associated unique chip identifier, and any associated unique device identity together with a certificate for the same, are stored by the secure processing point 150 in the permanent public database 170. This database is accessible to third parties, e.g. over the Internet. Thus, after a device has been assembled and shipped, a third party may, using e.g. the unique chip identifier of a device, retrieve the backup data package of the device. Since the backup data package is used to restore specific data that have been associated with the device, the backup data package will not be useful to a third party which is not the rightful possessor of the device. It should be noted that the public key of the public/private key pair associated with the secure communication channel could be stored in the public database so as to be accessible to a third party. In this case the secure communication channel will not only be a channel between

15

the device and the manufacturer, but between any party and the device.

After step 8 in the assembly process the device is ready for shipment, the shipment being illustrated by
5 arrow 9.

With reference to Fig. 2 some examples of possible device management activities are described that can be performed with respect to the assembled device after its shipment.

10 Fig. 2 includes the databases 160 and 170 previously described with reference to Fig. 1. Database 170 is the public database storing backup data packages and database 160 is the optional secret database storing various device specific secret data. The device 100 correspond to
15 the device assembled in Fig. 1 after shipment, now in control by its owner. The figure also shows a third party application server 180, operatively connected to the public database 170, and a device service server 190 operated by the device manufacturer and operatively
20 connected to the database 160 and 170 with device specific data.

Now, assume that the memory circuit 130 of the device for some reason loses its content. This implies that all cryptographic keys that were stored in the
25 device during assembly will be lost. Via a third party application server which interact with the public database 170 over, e.g. the Internet, the owner of the personal device will then be able to restore some of the lost data in the flash memory without any interaction
30 with a service point and/or a secret database.

The recovery of the essential flash memory data is achieved by first reading the unique chip identifier from the read-only storage 120 of the personal device 100. The chip identifier is then sent to an on-line system
35 incorporating the public database 170. The on-line system returns the corresponding backup data package and certificate for the unique device identity, without

16

having to access any secret information. The owner is then able to create a new flash image using the received copy of the backup data package and the certificate. When the device 100 then is booted up, the device will

5 recognize the backup code attached to the received backup data package and start to decrypt the backup data package to a data package which is identical to the data package originally stored in the flash memory during assembly of the device by the manufacturer. Moreover, the recovery

10 of the flash content also includes recovery of the unique device identity that has been allocated to the device. It should not be possible for anyone to change this device identity during a recovery, but it should be the same as that originally stored by the manufacturer. To ensure

15 this, the device uses the manufacturer's public signature key stored in the ROM memory of the device to verify the certificate and verify the authenticity of the device identity. This operation is thus performed without any interaction from the manufacturer. If this verification

20 is successful, the cryptographic keys and the unique device identity, and possibly some other data, which were associated with device during its assembly by the manufacturer, will be fully restored in the memory circuit 130.

25 If an owner of the device requests a service from the manufacturer, e.g. the downloading of new software modules, the owner accesses the device service server 190 provided by the manufacturer. The access includes transfer of the unique device identity of the device to

30 the server. The manufacturer's server 190 then retrieves or generates the appropriate cryptographic key corresponding to the received device identity and to be used for the secure communication with the device. Thus, such key may be a symmetric key retrieved from the

35 database 160, a symmetric key generated from the device identity and the master secret key, or a or a public key extracted from a certificate retrieved from database 170

17

with a corresponding private key stored in the device.
The applicable cryptographic key is then used for
encrypting the manufacturer's communication with device
using any appropriate operative connection. Typically
5 this is performed remotely, such as using a long distance
connection, the Internet, a wireless connection etc,
whichever is appropriate and supported by the interface
circuitry of the personal device. Thus, by means of the
secure communication channel with the personal device,
10 the manufacturer may provide various services with
respect to device, services that include downloading of
software modules, downloading of configuration data etc.

18

CLAIMS

1. A method for managing cryptographic keys that are specific to a personal device(100), the method being performed at a secure processing point(150) arranged in communication with the personal device, characterized in that the secure processing point performs the steps of:
- retrieving a unique chip identifier from a read-only storage(120) of an integrated circuit chip (110) included in the device (100);
- storing a data package in the device, the data package including at least one cryptographic key;
- receiving, in response to storing the data package, a backup data package from the device(100), which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage(125) of the chip (100);
- associating the unique chip identifier with the received backup data package; and
- storing the backup data package and the associated unique chip identifier in a permanent public database(170).
2. The method as claimed in claim 1, wherein the secure processing point performs the further steps of:
- associating a unique device identity with the unique chip identifier;
- signing the result of said associating step with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the device, thereby generating a certificate for the unique device identity;
- storing the certificate in the device; and
- storing the unique device identity and the certificate in association with the backup data package

and the unique chip identifier in the permanent public database.

3. The method as claimed in claim 1 or 2, wherein
5 the at least one cryptographic key includes at least one key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device.

10 4. The method as claimed in claim 3, wherein the at least one key to be used for a secure, key based communication channel includes a symmetric key.

5. The method as claimed in claim 4, wherein the
15 symmetric key is generated as a function of a master key and the unique device identity.

6. The method as claimed in any one of claims 3-5, wherein the at least one key to be used for a secure, key
20 based communication channel includes a private/public key pair.

7. The method as claimed in claim 6, wherein the private/public key pair either is:
25 generated by the secure processing point during assembly of the device; or
generated and stored in advance in a secure database before assembly of the device, in which latter case the cryptographic keys stored in advance of assembly are
30 removed from the secret database after reception of the backup data package.

8. The method as claimed in any one of claims 1-7, wherein the personal device is a wireless communications
35 terminal and the unique device identity an identifier which identifies the wireless communications terminal in a wireless communications network.

9. A system for managing cryptographic keys that are specific to a personal device, the system including at least one personal device(100) and a secure processing point(150), which secure processing point is arranged in communication with the personal device, c h a r a c t e r i s e d in that:

the device includes an integrated circuit chip(110) with a unique chip identifier in a read-only storage(120) and a unique secret chip key in a tamper-resistant secret storage(125);

the secure processing point includes processing means(155) for retrieving the unique chip identifier and for storing a data package in the device, the data package including at least one cryptographic key;

the device includes processing means(127) for encrypting the received data package with the unique secret chip key and transferring a resulting backup data package back to the secure processing point; and

the processing means of the secure processing point is arranged for storing the received backup data package in association with the unique chip identifier in a permanent public database(170).

10. The system as claimed in claim 9, wherein the processing means(155) of the secure processing point(150) further is arranged for:

associating a unique device identity with the unique chip identifier;

signing the result of the association with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the device, thereby generating a certificate for the unique device identity;

storing the certificate in the device; and
storing the unique device identity and the certificate in association with the backup data package

21

and the unique chip identifier in the permanent public database.

11. The system as claimed in claim 9 or 10, wherein
5 the at least one cryptographic key includes at least one key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device.

10 12. The system as claimed in claim 11, wherein the at least one key to be used for a secure, key based communication channel includes a symmetric key.

13. The system as claimed in claim 12, wherein the
15 symmetric key is generated as a function of a master key and the unique device identity.

14. The system as claimed in any one of claims 11-
13, wherein the at least one key to be used for a secure,
20 key based communication channel includes a private/public key pair.

15. The system as claimed in claim 14, wherein the
the processing means of the secure processing point
25 either is:

arranged for generating the private/public key pair during assembly of the device; or

arranged for retrieving the private/public key pair
from a secure database (140), in which the key pair has
30 been stored in advance before assembly of the device, in which latter case the secure processing point further is arranged for removing the key pair from the secret database after reception of the backup data package.

35 16. The system as claimed in any one of claims 9-15, wherein the personal device is a wireless communications terminal and the unique device identity an identifier

which identifies the wireless communications terminal in a wireless communications network.

17. A method of recovering a backup data package of
5 a personal device (100), which backup data package has been assembled and stored in accordance with any one of claims 1-8, the method including the steps of:
- reading a unique chip identifier from a read-only storage (120) of the personal device (100);
 - 10 transmitting the chip identifier to a public database (170);
 - receiving from the public database the backup data package corresponding to the transmitted chip identifier; and
 - 15 storing the received backup data package in the personal device.

18. A personal device(100) managing cryptographic keys that are specific to the personal device,
20 c h a r a c t e r i s e d in that the personal device includes:
- an integrated circuit chip(110) with a unique chip identifier in a read-only storage(120) and a unique secret chip key in a tamper-resistant secret
 - 25 storage(125);
 - processing means(127) for outputting the unique chip identifier;
 - memory means(130) for storing a received data package including at least one cryptographic key; and
 - 30 processing means(127) for encrypting the received data package with the unique secret chip key and outputting a resulting backup data package to a permanent public database(170).

- 35 19. The personal device as claimed in claim 18, wherein the personal device includes a read-only memory(120) storing a manufacturer public signature key

23

and the memory means(130) is further for storing a received certificate, which corresponds to a certificate stored in association with the backup data package in the public database and which has been signed with a
5 manufacturer private signature key corresponding to the manufacturer public signature key.

20. The personal device as claimed in claim 18 or 19, wherein the at least one cryptographic key includes
10 at least one key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device.

21. The personal device as claimed in claim 20,
15 wherein the at least one key to be used for a secure, key based communication channel includes a symmetric key.

22. The personal device as claimed in claim 21,
wherein the symmetric key is generated as a function of a
20 master key and the unique device identity.

23. The personal device as claimed in any one of claims 20-22, wherein the at least one key to be used for a secure, key based communication channel includes a
25 private/public key pair.

24. The personal device as claimed in any one of claims 18-23, wherein the personal device is a wireless communications terminal and the unique device identity an
30 identifier which identifies the wireless communications terminal in a wireless communications network.

25. A secure processing point(150) for managing cryptographic keys that are specific to personal devices,
35 the secure processing point being capable of communicating with a personal device(100),

24

characterised in that the secure processing point includes processing means(155) for:

retrieving a unique chip identifier from a read-only storage(120) of an integrated circuit chip(110) included
5 by the personal device(100);

storing a data package including at least one cryptographic key in the personal device;

receiving an encrypted version of the data package, in the form of a backup data package, from the personal
10 device in response to the stored data package; and

storing the received backup data package in association with the unique chip identifier in a permanent public database(170).

15 26. The secure processing point as claimed in claim 25, wherein the processing means(155) further is arranged for:

associating a unique device identity with the unique chip identifier;

20 signing the result of the association with a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the device, thereby generating a certificate for the unique device identity;

25 storing the certificate in the device; and
storing the unique device identity and the certificate in association with the backup data package and the unique chip identifier in the permanent public database.

30

25

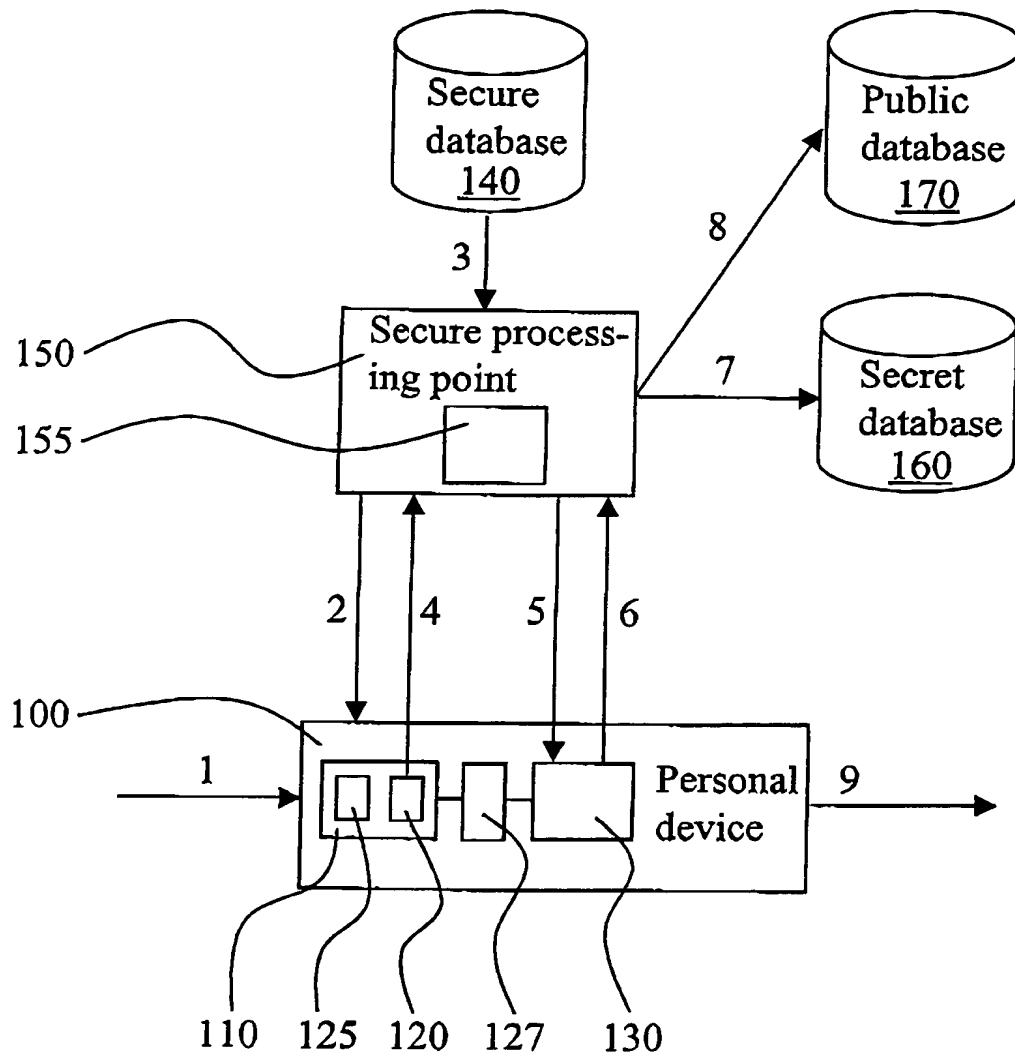
ABSTRACT

The present invention relates to key management of cryptographic keys, which keys are intended to be used by applications included in a personal device 100. According to the invention a data package including one or more cryptographic keys is transferred to a personal device 100 from a secure processing point 150 of a device assembly line in order to store device specific cryptographic keys in the personal device 100. In response to the transferred data package, a backup data package is received by the secure processing point 150 from the personal device 100, which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage 125 of a chip 110 included in the personal device 100. The secure processing point 150 is arranged to store the backup data package, together with an associated unique chip identifier read from the personal device 100, in a permanent, public database 170.

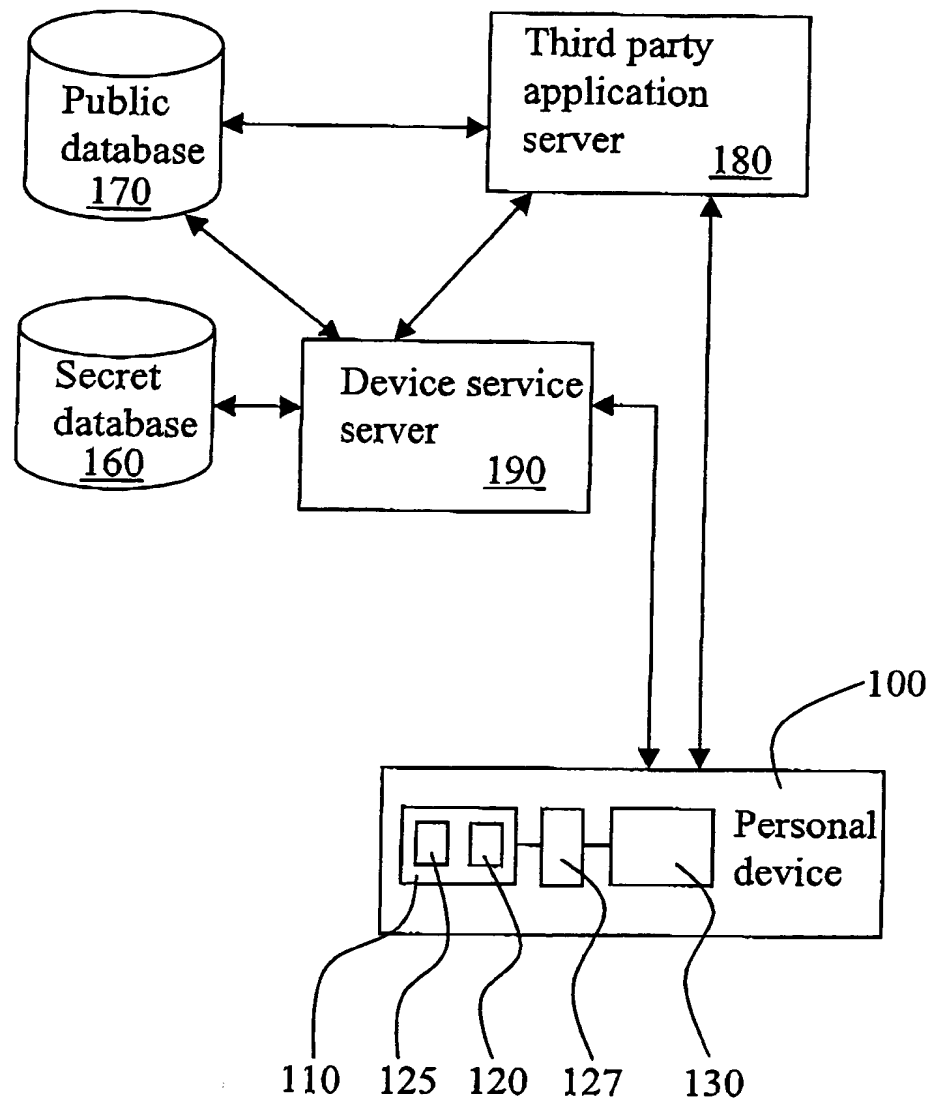
[Fig. 1]

A Ro

1/2

**FIG. 1**

2/2

**FIG. 2**